(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
29. August 2002 (29.08.2002)

PCT

(10) Internationale Veröffentlichungsnummer
WO 02/067191 A1

(51) Internationale Patentklassifikation[7]: G06K 19/073

(21) Internationales Aktenzeichen: PCT/EP02/00733

(22) Internationales Anmeldedatum:
24. Januar 2002 (24.01.2002)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
101 07 373.9 16. Februar 2001 (16.02.2001) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: INFINEON TECHNOLOGIES AG [DE/DE]; St.-Martin-Str. 53, 81669 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: JANKE, Marcus [DE/DE]; Spitzingplatz 3, 81539 München (DE).

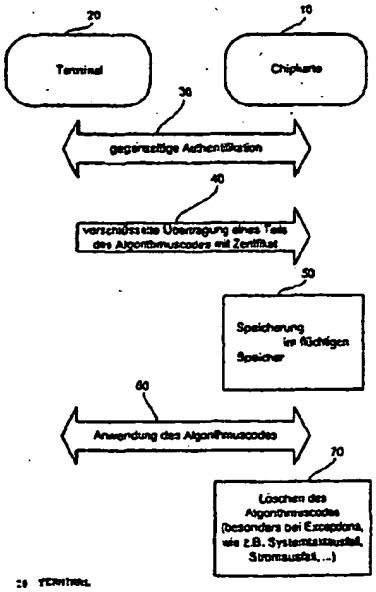
(74) Anwälte: SCHOPPE, Fritz usw.; Schoppe, Zimmermann, Stöckeler & Zinkler, Postfach 71 08 67, 81458 München (DE).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

[Fortsetzung auf der nächsten Seite]

(54) Title: SECURITY MODULE COMPRISING A VOLATILE MEMORY FOR STORING AN ALGORITHM CODE

(54) Bezeichnung: SICHERHEITSMODUL MIT FLÜCHTIGEM SPEICHER ZUR SPEICHERUNG EINES ALGORITHMUS-CODES



10 TERMINAL
10 CHIP CARD
30 MUTUAL AUTHENTICATION
40 ENCRYPTED TRANSMISSION OF A PORTION OF THE ALGORITHM CODE WITH CERTIFICATE
50 STORAGE IN THE VOLATILE MEMORY
60 USE OF THE ALGORITHM CODE
70 DELETION OF THE ALGORITHM CODE (PARTICULARLY IN THE CASE OF EXCEPTIONS SUCH AS SYSTEM CLOCK FAILURE, POWER FAILURE, ...)

(57) Abstract: The invention relates to a security module (100) for use with a terminal. The security module comprises a data interface (110), which can be coupled to a terminal and which is provided for receiving at least one portion of an algorithm code or the entire algorithm code from the terminal. The security module also comprises a power interface (120) for receiving supply power. A volatile memory (130), which is coupled to the power interface (120) in order to be supplied with power, stores the portion of the algorithm code or the entire algorithm code that is received via the data interface. A processor (140) executes the algorithm code in order to obtain an algorithm code outcome that can be supplied to the terminal. The algorithm code of the security module (100) is effectively protected from spying conducted by a potential hacker due to the storing of at least one portion of an algorithm code in the volatile memory (130) of the security module (100) as described by the invention.

(57) Zusammenfassung: Ein Sicherheitsmodul (100) zur Verwendung mit einem Terminal umfaßt eine Datenschnittstelle (110), die mit einem Terminal koppelbar ist, zum Empfangen zumindest eines Teils eines Algorithmuscodes oder des vollständigen Algorithmuscodes von dem Terminal sowie eine Energieschnittstelle (120) zum Empfangen von Versorgungsenergie. Ein flüchtiger Speicher (130), der mit der Energieschnittstelle (120) gekoppelt ist, um mit Energie versorgt zu werden, speichert den über die Datenschnittstelle empfangenen Teil des Algorithmuscodes oder den vollständigen Algorithmuscode, wobei ein Prozessor (140) den Algorithmuscode ausführt, um ein Algorithmuscodeergebnis zu erhalten, das zu dem Terminal lieferbar ist. Durch die erfindungsgemäße Speicherung zumindest eines Teils eines Algorithmuscodes in dem flüchtigen Speicher (130) des Sicherheitsmoduls (100) wird der Algorithmuscode des Sicherheitsmoduls (100) wirksam vor einem Ausspähen durch einen potentiellen Angreifer geschützt.

WO 02/067191 A1

(84) **Bestimmungsstaaten** *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist: Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.